⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－293580

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開 昭和63年(1988)11月30日
G 09 C 1/00		7368－5B	
G 06 F 12/00	302	U－8841－5B	
12/14	320	B－7737－5B	審査請求 未請求 発明の数 1 （全10頁）

⑤4発明の名称　表形式データ暗号化方式

⑳特　願　昭62－130786
㉒出　願　昭62(1987)5月26日

⑦2発 明 者　北澤　具子　東京都港区芝5丁目33番1号　日本電気株式会社内
⑦1出 願 人　日本電気株式会社　東京都港区芝5丁目33番1号
⑦4代 理 人　弁理士 河原 純一

明　細　書

1．発明の名称

表形式データ暗号化方式

2．特許請求の範囲

表単位に異なる暗号化のための定義情報を入力する定義情報入力手段と、

この定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビットを反転するビット反転手段と、

前記定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビット位置を変換するビット位置変換手段と、

前記ビット反転手段と前記ビット位置変換手段とによって基準コードテーブルから暗号テーブルを作成する暗号テーブル作成手段と、

この暗号テーブル作成手段により作成された暗号テーブルから解読テーブルを作成する解読テーブル作成手段と、

表形式データの暗号化時に暗号化する表形式データを入力するデータ入力手段と、

このデータ入力手段により入力された表形式データを前記暗号テーブル作成手段によって作成された暗号テーブルに従って暗号化するデータ暗号化手段と、

このデータ暗号化手段により暗号化された表形式データを出力する暗号化データ出力手段と、

暗号化された表形式データの解読時に暗号化された表形式データを入力する暗号化データ入力手段と、

この暗号化データ入力手段により入力された暗号化された表形式データを前記解読テーブル作成手段によって作成された解読テーブルに従って解読するデータ解読手段と、

このデータ解読手段により解読された表形式データを出力するデータ出力手段と、

を有することを特徴とする表形式データ暗号化方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は表形式データ暗号化方式に関し、特に表形式データをファイル中の表サブファイルに書き込む際のデータの暗号化および表サブファイルから表形式データを読み込む際のデータの解読を行う表形式データ暗号化方式に関する。

〔従来の技術〕

従来、この種の表形式データ暗号化方式としては、プログラム中に固定的に持たれたコード変換表によって表形式データの暗号化を行う方法や、外部記憶装置に固定的に持たれたコード変換表を入力して表形式データの暗号化を行う方法などがあった。

〔発明が解決しようとする問題点〕

上述した従来の表形式データ暗号化方式は、固定的に持たれたコード変換表を用いて表形式データの暗号化および解読を行うようになっていたので、コード変換表があれば暗号化された表形式データが容易に解読されてしまう欠点がある。

本発明の目的は、上述の点に鑑み、ファイル中の表サブファイルに書き込まれた表形式データが容易に解読されることがないようにした表形式データ暗号化方式を提供することにある。

〔問題点を解決するための手段〕

本発明の表形式データ暗号化方式は、表単位に異なる暗号化のための定義情報を入力する定義情報入力手段と、この定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビットを反転するビット反転手段と、前記定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビット位置を変換するビット位置変換手段と、前記ビット反転手段と前記ビット位置変換手段とによって基準コードテーブルから暗号テーブルを作成する暗号テーブル作成手段と、この暗号テーブル作成手段により作成された暗号テーブルから解読テーブルを作成する解読テーブル作成手段と、表形式データの暗号化時に暗号化する表形式データを入力するデータ入力手段と、このデータ入力手段により入力された表形式データを前記暗号テーブル作成手段によって作成された暗号テーブルに従って暗号化するデータ暗号化手段と、このデータ暗号化手段により暗号化された表形式データを出力する暗号化データ出力手段と、暗号化された表形式データの解読時に暗号化された表形式データを入力する暗号化データ入力手段と、この暗号化データ入力手段により入力された暗号化された表形式データを前記解読テーブル作成手段によって作成された解読テーブルに従って解読するデータ解読手段と、このデータ解読手段により解読された表形式データを出力するデータ出力手段とを有する。

〔作用〕

本発明の表形式データ暗号化方式では、定義情報入力手段が表単位に異なる暗号化のための定義情報を入力し、ビット反転手段が定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビットを反転し、ビット位置変換手段が定義情報入力手段により入力された該当する表の暗号の定義情報に基づいて基準コードテーブルのコードのビット位置を変換し、暗号テーブル作成手段がビット反転手段とビット位置変換手段とによって基準コードテーブルから暗号テーブルを作成し、解読テーブル作成手段が暗号テーブル作成手段により作成された暗号テーブルから解読テーブルを作成し、データ入力手段が表形式データの暗号化時に暗号化する表形式データを入力し、データ暗号化手段がデータ入力手段により入力された表形式データを暗号テーブル作成手段によって作成された暗号テーブルに従って暗号化し、暗号化データ出力手段がデータ暗号化手段により暗号化された表形式データを出力し、暗号化データ入力手段が暗号化された表形式データの解読時に暗号化された表形式データを入力し、データ解読手段が暗号化データ入力手段により入力された暗号化された表形式データを解読テーブル作成手段によって作成された解読テーブルに従って解読し、データ出力手段がデータ解読手段により解読された表形式データを出力する。

（実施例）

次に、本発明について図面を参照して詳細に説明する。

第１図は、本発明の表形式データ暗号化方式の一実施例の構成を示すブロック図である。本実施例の表形式データ暗号化方式は、表サブファイル17ａを格納するファイル17と、ファイル17中の表サブファイル17ａのオープン時に暗号テーブル13と解読テーブル14とを作成する表サブファイルオープン処理部100 と、表形式データ15をファイル17中の表サブファイル17ａに書き込むときに表形式データ15を暗号テーブル13に基づいて暗号化するデータ暗号化処理部200 と、ファイル17中の表サブファイル17ａから暗号化された表形式データ18を読み込むときに暗号化された表形式データ18を解読テーブル14に基づいて解読するデータ解読処理部300 とから、その主要部が構成されている。

表サブファイルオープン処理部100 は、該当する表の暗号化のための定義情報12を入力する定義情報入力手段１と、定義情報入力手段１によって入力された該当する表の暗号化のための定義情報12を基に第５図に示す８ビットの組合せの全ケースである 256バイトの全コードを昇順に並べたテーブル（以下、基準コードテーブルと称する）の各コードの１バイト中のある位置のビットを反転させるビット反転手段３および基準コードテーブルの各コードの１バイト中のビットの位置を入れ替えるビット位置変換手段２を用いて 256バイトの全コードを暗号化したときのコード変換表である暗号テーブル13を作成する暗号テーブル作成手段４と、暗号テーブル作成手段４により作成された暗号テーブル13を基に 256バイトの全コードを解読したときのコード変換表である解読テーブル14を作成する解読テーブル作成手段５とを含んで構成されている。

データ暗号化処理部200 は、表形式データ15を入力するデータ入力手段６と、データ入力手段６により暗号化する表形式データ15を入力し暗号テーブル作成手段４によって作成された 256バイトの暗号テーブル13を用いて入力した表形式データ15を１バイト単位で暗号テーブル13中の対応するコードに置き換えて暗号化するデータ暗号化手段７と、データ暗号化手段７により暗号化された表形式データ16をファイル17中の表サブファイル17ａに書き込む暗号化データ出力手段８とを含んで構成されている。

データ解読処理部300 は、ファイル17中の表サブファイル17ａから暗号化された表形式データ18を入力する暗号化データ入力手段９と、暗号化データ入力手段９によりファイル17中の表サブファイル17ａから暗号化された表形式データ18を読み込み解読テーブル作成手段５によって作成された 256 バイトの解読テーブル14を用いて読み込んだ暗号化された表形式データ18を１バイト単位で解読テーブル14中の対応するコードに置き換えて解読するデータ解読手段10と、解読された表形式データ19を出力するデータ出力手段11とを含んで構成されている。

表形式データ15，16，18および19は可変長データであり、例えば第２図に表形式データ15を例にとって示すように、データの全バイト長15ａおよびフィールド数15ｂからなる制御部15ｃと、フィールド長15ｄおよびフィールド長15ｄ分のフィールドデータ15ｅの繰返しからなるデータ部15ｆとから構成されている。

第３図を参照すると、定義情報12は、１バイト中の左からのビットの順序に対応してそれぞれ移動先のビットの位置を指定している０から７までの順列であるビット位置変換情報12ａと、１バイト中の左からのビットの順序に対応してオン（１）は反転する、オフ（０）は反転しないことを意味するオンおよびオフの８ビットの組合せで反転するビットを指定しているビット反転情報12ｂとから構成されている。

次に、このように構成された本実施例の表形式データ暗号化方式の動作について説明する。

まず、ファイル17中の表サブファイル17ａに対する表形式データの入出力に先立って、表サブファイルオープン処理部100 が起動されてファイル17中の表サブファイル17ａのオープン処理が行わ

れる。このとき、暗号化に用いる暗号テーブル13と解読に用いる解読テーブル14との作成も同時に行われる。

定義情報入力手段１によって該当する表をどのように暗号化するかを規定する定義情報12が入力される。定義情報12は、表ごとに異なる定義を与えることが可能である。なお、本実施例では、具体的に第４図に示す定義情報12が入力されたものとして説明を行う。

１バイトのデータは、８ビットの組合せとして００００００００（２進）から１１１１１１１１（２進）までの２の８乗、つまり 256の組合せがあるが、この 256の組合せを昇順に並べると先頭からの変位と、その変位にある１バイトの値とが一致する第５図に示すような基準コードテーブルが得られる。この基準コードテーブルを第４図に示した定義情報12により暗号テーブル13に変換する。つまり、暗号テーブル13は、暗号テーブル13の先頭から何バイト目にあるかという変位が暗号化される前の１バイトのコードの値を示すことになる。

まず、第４図に示した定義情報12に基づいてビット位置変換手段２を用いてビット位置の変換を行うが、 256バイトを昇順に並べた基準コードテーブル中の、例えばＣ１（16進）のコードがどのように暗号テーブル13のコードに変換されるかが第９図に示されている。定義情報12では、０ビット目を４ビット目に、１ビット目を５ビット目に、２ビット目を６ビット目に、３ビット目を７ビット目に、４ビット目を０ビット目に、５ビット目を１ビット目に、６ビット目を２ビット目に、７ビット目を３ビット目にそれぞれ置き換える指定なので、ビット位置の変換をビット位置変換手段２を用いて行うと、第９図に示すように、Ｃ１（16進）のコードは１Ｃ（16進）になる。さらに、この１Ｃ（16進）に対してビット反転手段３を用いて定義情報12に指定されているように０ビット目と４ビット目とを反転するとコードは９４（16進）となり、これが暗号テーブル13の変位Ｃ１（16進）に対応する暗号コードとなる。この変換を第５図の 256バイト全てについて行うと、まずビット位置変換手段２によって第６図に示すテーブルとなり、さらにビット反転手段３によって第７図に示す暗号テーブル13が完成する。

なお、本実施例では、先にビット位置変換手段２によるビット位置変換処理を行い、次にビット反転手段３によるビット反転処理を行ったが、この順序を入れ替えて先にビット反転手段３によるビット反転処理を行い、次にビット位置変換手段２によるビット位置変換処理を行う方法もある。

解読テーブル作成手段５では、暗号化された表形式データ18を解読するための解読テーブル14を作成するが、この解読テーブル14は暗号テーブル13を用いて作成する。暗号テーブル13は、暗号テーブル13の先頭からの変位の値をもつ１バイトのコードをその変位にある１バイトの値と入れ換えて暗号化するので、解読テーブル14は、第10図に示すように、暗号化された１バイトの値の変位にある１バイトのコードを変位とし変位を解読されたコードとしておけば解読できることになる。そこで、暗号テーブル13の 256バイトについて、暗号テーブル13の先頭からの変位の値を暗号テーブル13のその変位にある１バイトの値と一致する解読テーブル14の変位に１バイトのコードとして入れていけば、第８図に示すような解読テーブル14が作成できる。

次に、表形式データ15の暗号化を行うためにデータ暗号化処理部200 が起動されると、まず暗号化する表形式データ15がデータ入力手段６を用いて入力される。入力された表形式データ15は、データ暗号化手段７により暗号テーブル13を用いて暗号化されるが、入力された表形式データ15のデータ部15ｆのみが暗号化される。表形式データ15の制御部15ｃについては、暗号化するときおよび解読するときにデータ部15ｆの全バイト長15ａが必要であるために暗号化しない。表形式データ15のデータ部15ｆを１バイトずつにして、暗号テーブル13のその１バイトの値の変位にあるコードに置き換える。

例えば、第11図に示すように、データ部15ｃが

０２Ｃ１Ｃ２０１Ｃ３（16進）というデータが入力されたとすると、まず０２は第７図に示す暗号テーブル13の変位０２（16進）にあるコードＡ８（16進）と置き換え、Ｃ１は暗号テーブル13の変位Ｃ１（16進）にあるコード９４（16進）と置き換え、Ｃ２は暗号テーブル13の変位Ｃ２（16進）にあるコードＡ４（16進）と置き換え、０１は暗号テーブル13の変位０１（16進）にあるコード９８（16進）と置き換え、Ｃ３は暗号テーブル13の変位Ｃ３（16進）にあるコードＢ４（16進）と置き換えることによって、データ部０２Ｃ１Ｃ２０１Ｃ３（16進）は、Ａ８９４Ａ４９８Ｂ４（16進）と暗号化される。

このようにして暗号化された表形式データ16は、暗号化データ出力手段８によってファイル17中の表サブファイル17ａに書き込まれる。本実施例の表形式データ暗号化方式では、可変長の表形式データ15のデータ部15ｆをフィールド長15ｄを含めて暗号化することによって、より一層暗号化の効果があがるようになっている。

続いて、ファイル17中の表サブファイル17ａに書き込まれたデータを解読するためにデータ解読処理部300が起動されると、まず暗号化された表形式データ18を暗号化データ入力手段９を用いてファイル17中の表サブファイル17ａから読み込む。読み込まれた暗号化された表形式データ18は、データ解読手段10によって解読されるが、暗号化された表形式データ18を１バイトずつにしてそれぞれ解読テーブル14のその１バイトの値の変位にあるコードに置き換える。

例えば、第12図に示すＡ８９４Ａ４９８Ｂ４（16進）という暗号化された表形式データ18のデータ部を解読すると、まずＡ８（16進）は第８図に示す解読テーブル14の変位Ａ８（16進）にあるコード０２（16進）と置き換え、９４（16進）は解読テーブル14の変位９４（16進）にあるコードＣ１（16進）と置き換え、Ａ４（16進）は解読テーブル14の変位Ａ４（16進）にあるコードＣ２（16進）と置き換え、９８（16進）は解読テーブル14の変位９８（16進）にあるコード０１（16進）と置き換え、Ｂ４（16進）は解読テーブル14の変位Ｂ４（16進）にあるコードＣ３（16進）と置き換えることによって、暗号化された表形式データ18のデータ部Ａ８９４Ａ４９８Ｂ４（16進）は０２Ｃ１Ｃ２０１Ｃ３（16進）と解読される。

第11図および第12図の例は、表形式データ15のデータ部15ｆを暗号化しＡ８９４Ａ４９８Ｂ４（16進）となり、それを解読して元の表形式データ15のデータ部15ｆと同一の表形式データ18のデータ部０２Ｃ１Ｃ２０１Ｃ３（16進）を得たことになる。

（発明の効果）

以上説明したように本発明は、表単位に暗号化のための定義情報を与えて暗号化および解読の際に使用されるコード変換表である暗号テーブルおよび解読テーブルを定義情報から動的に作成することにより、コード変換表を固定的に持つ場合に比べて暗号化された表形式データの解読が格段的に困難になり、機密保護に効果がある。特に、表形式データのデータ部のフィールド長も含めて暗号化を行えるので、さらに機密保護に効果がある。

４．図面の簡単な説明

第１図は本発明の一実施例の構成を示すブロック図、

第２図は第１図中の表形式データの構成を示す図、

第３図は第１図中の定義情報の構成を示す図、

第４図は第３図に示した定義情報の具体例を示す図、

第５図は256バイトのコードを昇順に並べた基準コードテーブルを示す図、

第６図は第５図に示した基準コードテーブルに対して第１図中のビット位置変換手段によりビット位置変換処理を実行して得られたテーブルを示す図、

第７図は第６図に示したテーブルに第１図中のビット反転手段によりビット反転処理を実行して得られた暗号テーブルを示す図、

第８図は第７図に示した暗号テーブルから第１図中の解読テーブル作成手段により作成された解

読テーブルを示す図、

第９図は第５図に示した基準コードテーブルを第７図に示した暗号テーブルに変換する処理の一例を示す図、

第10図は第７図に示した暗号テーブルから第８図に示した解読テーブルを作成する処理の一例を示す図、

第11図は表形式データを第７図に示した暗号テーブルを用いて暗号化する処理の一例を示す図、

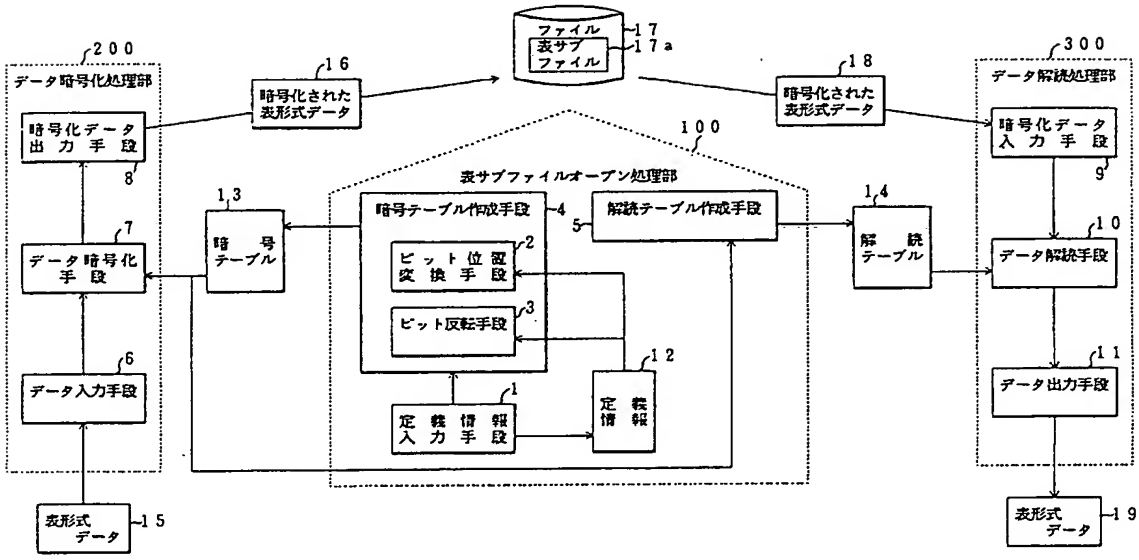
第12図は表形式データを第８図に示した解読テーブルを用いて解読する処理の一例を示す図である。

図において、

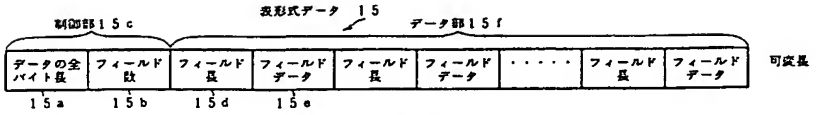
１・・・定義情報入力手段、
２・・・ビット位置変換手段、
３・・・ビット反転手段、
４・・・暗号テーブル作成手段、
５・・・解読テーブル作成手段、
６・・・データ入力手段、
７・・・データ暗号化手段、
８・・・暗号化データ出力手段、
９・・・暗号化データ入力手段、
10・・・データ解読手段、
11・・・データ出力手段、
12・・・定義情報、
13・・・暗号テーブル、
14・・・解読テーブル、
15・・・表形式データ、
16・・・暗号化された表形式データ、
17・・・ファイル、
17a・・表サブファイル、
18・・・暗号化された表形式データ、
19・・・表形式データである。

特許出願人　日本電気株式会社
代理人　弁理士　河原純一

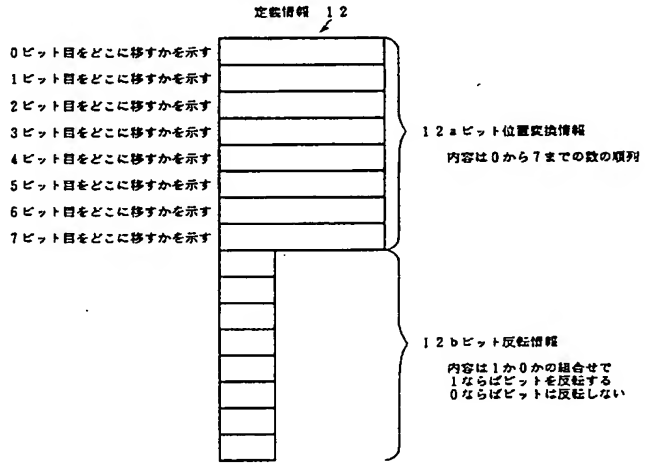
第１図



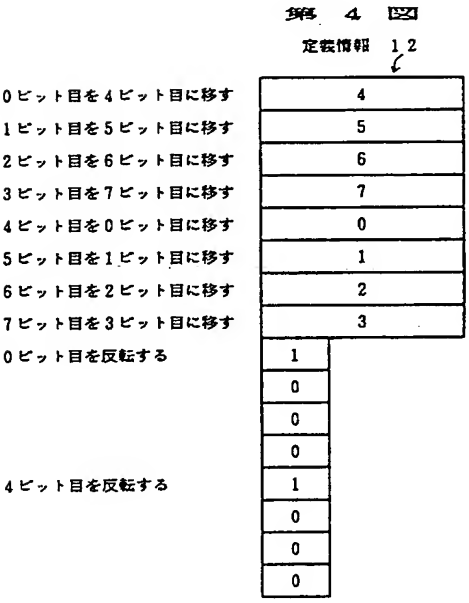
第２図


表形式データ　１５
制御部１５ｃ
データ部１５ｆ
データの全バイト長
フィールド数
フィールド長
フィールドデータ
フィールド長
フィールドデータ
・・・・・
フィールド長
フィールドデータ
可変長
１５ａ
１５ｂ
１５ｄ
１５ｅ

第３図


定義情報　１２
０ビット目をどこに移すかを示す
１ビット目をどこに移すかを示す
２ビット目をどこに移すかを示す
３ビット目をどこに移すかを示す
４ビット目をどこに移すかを示す
５ビット目をどこに移すかを示す
６ビット目をどこに移すかを示す
７ビット目をどこに移すかを示す
１２ａビット位置変換情報
内容は０から７までの数の順列
１２ｂビット反転情報
内容は１か０かの組合せで
１ならばビットを反転する
０ならばビットに反転しない

第４図


定義情報　１２
０ビット目を４ビット目に移す　4
１ビット目を５ビット目に移す　5
２ビット目を６ビット目に移す　6
３ビット目を７ビット目に移す　7
４ビット目を０ビット目に移す　0
５ビット目を１ビット目に移す　1
６ビット目を２ビット目に移す　2
７ビット目を３ビット目に移す　3
０ビット目を反転する　1
0
0
0
４ビット目を反転する　1
0
0
0

第 5 図

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

２５６バイトのコードを昇順に並べた基準コードテーブル（１６進にて表示）
基準コードテーブルの先頭からの変位とその変位にある１バイトの値とは一致する

第 6 図

001020304050607080 90A0B0C0D0E0F001112131415161718191A1B1C1D1E1F1
021222324252627282 92A2B2C2D2E2F203132333435363738393A3B3C3D3E3F3
041424344454647484 94A4B4C4D4E4F405152535455565758595A5B5C5D5E5F5
061626364656667686 96A6B6C6D6E6F607172737475767778797A7B7C7D7E7F7
081828384858687888 98A8B8C8D8E8F809192939495969798999A9B9C9D9E9F9
0A1A2A3A4A5A6A7A8A 9AAABACADAEAFA0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFB
0C1C2C3C4C5C6C7C8C 9CACBCCCDCECFC0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFD
0E1E2E3E4E5E6E7E8E 9EAEBECEDEEEFE0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFFF

２５６バイトのコードを昇順に並べた基準コードテーブル（第５図）にビット位置変換手段２を
実行してビット位置を変換して得られたテーブル

第 7 図

8898A8B8C8D8E8F8081828384858687888999A9B9C9D9E9F9091929394959697 9
8A9AAABACADAEAFA0A1A2A3A4A5A6A7A8B9BABBBCBDBEBFB0B1B2B3B4B5B6B7B
8C9CACBCCCDCECFC0C1C2C3C4C5C6C7C8D9DADBDCDDDEDFD0D1D2D3D4D5D6D7D
8E9EAEBECEDEEEFE0E1E2E3E4E5E6E7E8F9FAFBFCFDFEFFF0F1F2F3F4F5F6F7F
8090A0B0C0D0E0F000102030405060708191A1B1C1D1E1F101112131415161 71
8292A2B2C2D2E2F202122232425262728393A3B3C3D3E3F303132333435363 73
8494A4B4C4D4E4F404142434445464748595A5B5C5D5E5F505152535455556 575
8696A6B6C6D6E6F606162636465666768797A7B7C7D7E7F707172737475767 77

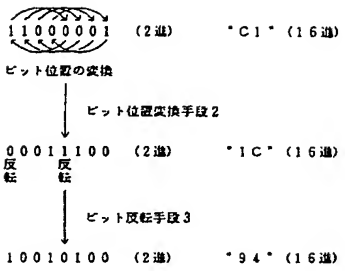
第６図のビット位置変換手段２を実行して得られたテーブルに対して
ビット反転手段３を実行して完成した暗号テーブル１３

第 8 図

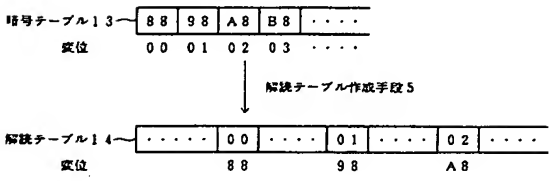
8898A8B8C8D8E8F8081828384858687888999A9B9C9D9E9F9091929394959697 9
8A9AAABACADAEAFA0A1A2A3A4A5A6A7A8B9BABBBCBDBEBFB0B1B2B3B4B5B6B7B
8C9CACBCCCDCECFC0C1C2C3C4C5C6C7C8D9DADBDCDDDEDFD0D1D2D3D4D5D6D7D
8E9EAEBECEDEEEFE0E1E2E3E4E5E6E7E8F9FAFBFCFDFEFFF0F1F2F3F4F5F6F7F
8090A0B0C0D0E0F000102030405060708191A1B1C1D1E1F101112131415161 71
8292A2B2C2D2E2F202122232425262728393A3B3C3D3E3F303132333435363 73
8494A4B4C4D4E4F404142434445464748595A5B5C5D5E5F505152535455556 575
8696A6B6C6D6E6F606162636465666768797A7B7C7D7E7F707172737475767 77

第７図の暗号テーブル１３から作成した解読テーブル１４

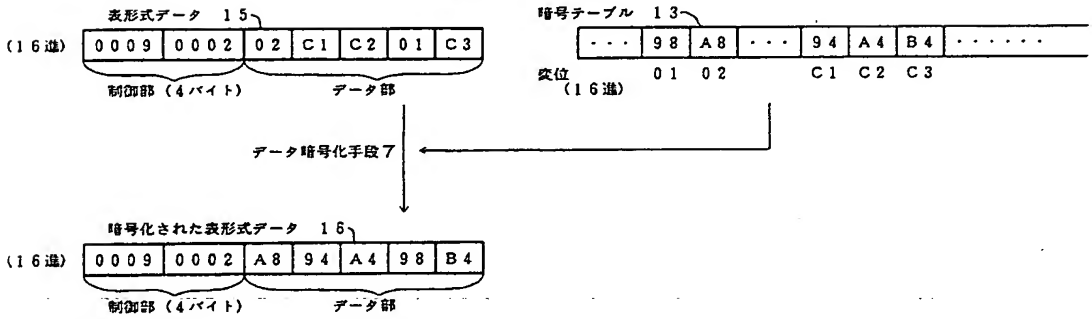
第 9 図



第 10 図



第 11 図



第 12 図